This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Security Deployment Guide

Role-Based Access Control

4/23/2026

Role-Based Access Control

Contents

> **Warning**
> Role-Based Access Control is complementary to Object-Based Access Control. Appropriate object permissions should be defined before setting up role-based access privileges.

Role-Based Access Control provides an additional layer of protection of your data from unauthorized users by defining what is displayed in the interface and therefore limiting the data to which a user has access.

> **Important**
> In this section, the term user is intended to mean both an individual user and Access Groups. This feature applies to both object types.

Roles enhance object-based access control by limiting the visibility of sets of configuration objects, and allowing you to tune elementary permissions to those objects to a finer level. For example, elementary permissions might indicate that you can write to an object, but roles can be used to restrict writing to an individual property of that object, such as **Name**.

Roles can also be used to protect access to entities that are not represented by configuration objects, such as tracking and troubleshooting information. Elementary permissions do not protect these entities, but it is logical to expect that unlimited access to them is not desirable.

Security Benefits

Permissions alone protect access to all parts of individual objects. In other words, once a user has access to an object, he or she has access to all properties of that object. Role-Based Access Control enables you to fine tune access to your data so that individual properties of objects are also protected. A user's permissions might allow that user to access an object, but roles limit what properties of the object the user can see and what the user can do to those properties. Roles also limit access to resources and functionality beyond configuration. In other words, access to an object can be modified without reconfiguring the object.

Furthermore, roles limit access to resources and functionality. Because roles affect what is displayed to the user, a user will not be made aware of functionality unless it is appropriate to their responsibilities.

Supporting Components

Role-Based Access Control is supported by the following components:

- Management Framework
- Genesys Administrator
- Genesys Administrator Extension

This feature is used by the following components:

- Genesys Administrator, on behalf of Management Framework and Outbound Contact
- Interaction Workspace
- Universal Contact Server
- Knowledge Manager

In addition, Platform SDK provides access to configuration objects needed to implement Role-Based Access Control in an application. For details about how this feature can be used in custom-built applications, refer to the appropriate API Reference for your development platform.

Feature Description

The major component of Role-Based Access Control is a *role*. Roles define what facilities are provided to users to review and manipulate various types of data. These include which property controls are available for items permitted by object permissions, what modules are visible, and access control for entities not represented by configuration objects. A role is assigned to a user, and that user is then able to do only what that role permits.

> **Important**
>
> One user can be assigned multiple roles, and one role can be assigned to multiple users.

Roles consist of a set of *role privileges*. Role privileges are tasks that can be performed on a given type of data. They are pre-defined in Genesys Administrator and are unique to each product. By default, any role privilege is not assigned to any role, so you must explicitly assign privileges to roles. Role privileges range from general to very specific tasks. An authorized user, normally a System Administrator, bundles these tasks into roles. These roles are then assigned to users. As a result, each user can perform only those tasks for which they have the privileges.

Role-Based Access is enforced primarily by visibility in the interface. When a user logs into an interface that supports roles, what that user sees is determined by the roles which have been assigned. If the user is not assigned a role that grants them access to a piece of functionality, that functionality will not be displayed to the user.

Roles vs. Permissions

Roles are intended to work with permissions to more finely tune what a user in your system can access.

Elementary permissions protect access to a whole object. That is, the permissions applied to the object apply equally to all properties of the object. There is no way to limit access to an individual property of that object. In addition, permissions do not restrict access to any parts of the object - if you have access permissions, you see the entire object.

Roles serve to protect properties of an object by hiding or disabling those properties for which a user should not have access. Different roles can define different access and allowed functionality for the same objects. In essence, roles resolve both problems with using permissions alone—the user can access and work with only those parts of the object to which that user is allowed.

Roles can also be used to protect access to entities that are not configured as configuration objects, such as logs.

In general, when determining the accessibility of an object to a user, the user session cannot retrieve objects if they are not among those objects to which the user has access (as defined by object-access permissions). Then, for that data that is available in the session, role privileges refine what can be done with the data. For example, if the user's permissions do not allow any Change permissions for a set of objects, that user cannot make any changes to those objects regardless of what his or her role privileges are for tasks for properties of those objects.

Multiple Roles

You can assign more than one role to a user. In such cases, the user will have the combined set of privileges granted by each role. In other words, the user is granted any privilege that is granted by at least one of the assigned roles. This ensures that the user is able to perform the tasks of all roles in which they participate.

New Users

By default, new users are not assigned any default roles. They must be assigned roles by a System Administrator or by an existing user with appropriate privileges.

Feature Configuration

> **Important**
> To determine if this section applies to you, see Supporting Components.

Role-Based Access Control is configured in Genesys Administrator. You can create a role, give it a name, and assign it to users in Configuration Manager, but the role privileges can be defined only in Genesys Administrator. Configuration Manager itself does not support the feature.

Configuring Role-Based Access Control

To configure Role-based Access Control, use the following steps: **[+] Show steps**

1. In Genesys Administrator, go to **Provisioning** > **Accounts** > **Roles**.
2. If required, navigate to the folder in which you want to store the new Role.
3. Click **New**.
4. In the **General** section of the **Configuration** tab, enter information in the following fields:
   a. **Name**—The name of this Role. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   b. **Description**—(Optional) A description of this Role.
   c. **Tenant**—This field appears only in a multi-tenant environment, and indicates the Tenant to which this Role belongs. This value is set automatically, and you cannot change it.
   d. **State**—This field is enabled by default.
5. In the **Members** section of the **Configuration** tab, enter the Users and/or Access Groups to whom the Role is to be assigned.

> **Important**
>
> You can complete this step either now or later. If you decide to complete it later, use the steps in Assigning Existing Roles to Existing Users and Existing Access Groups.

6. On the **Role Privileges** tab, define the privileges to be granted by this Role, as follows:
   a. Select the products for which you want to include privileges in the Role. Only installed products that support Role-Based Access Control are listed.
   b. For each privilege, set its value to one of the following:
      - **Unassigned**—(Default) This privilege is not granted by this Role. However, if multiple Roles are assigned to the same User or Access Group, this setting is overridden if another Role sets this privilege as Allowed.
      - **Allowed**—This privilege is explicitly granted by this Role.
7. To save the new Role and register it in the Configuration Database, do one of the following:
   - Click **Save and Close** to return to the list of Roles.
   - Click **Save** to continue configuring the Role.
   - Click **Save and New** to save the new Role and start creating another one.

   If you have assigned this Role to any Users or Access Groups, a configuration dialog box will appear notifying you that Read access for this Role object will be granted to those Users and Access Groups.
8. Click **Yes**.

Assigning Roles

To assign roles to users and Access Groups, use the following steps: **[+] Show steps**

Prerequisites

- The Roles to be assigned, and the Users or Access Groups to which they are to be assigned must exist in the Configuration Database.

Start of procedure

1. Log in to Genesys Administrator, if necessary. You can assign Roles to Users and Access Groups from three locations: Roles, Users, and Access Groups. The following steps describe each of these approaches.
2. Starting from Role objects: To assign one or more Roles to one or more Users or Access Groups, do the following:
   a. Go to **Provisioning** > **Accounts** > **Roles**.
   b. If necessary, navigate to the folder that contains the Roles you want to assign.
   c. Select one or more Roles.
   d. Open the **Tasks** panel, if necessary, and click **Assign Users** or **Assign Access Groups**, as appropriate, in the **User Access** section.
   e. Follow the steps in the **Role Management Wizard** to select the required Users or Access Groups and assign the Roles to them.
3. Starting from User objects: To assign one or more Roles to one or more Users, do the following:
   a. Go to **Provisioning** > **Accounts** > **Users**.
   b. If necessary, navigate to the folder that contains the Users to whom you want to assign Roles.
   c. Select one or more Users.
   d. Open the **Tasks** panel, if necessary, and click **Assign Roles** in the **User Access** section.
   e. Follow the steps in the **User Management Wizard** to select and assign the Roles.
4. Starting from Access Group objects: To assign one or more Roles to one or more Access Groups, do the following:
   a. Go to **Provisioning** > **Accounts** > **Access Groups**.
   b. If necessary, navigate to the folder that contains the Access Groups to whom you want to assign Roles.
   c. Select one or more Access Groups.
   d. Open the **Tasks** panel, if necessary, and click **Assign Roles** in the **User Access** section.
   e. Follow the steps in the **User Management Wizard** to select and assign the Roles.

End of procedure

Removing Roles

To remove (unassign) Roles from Users or Access groups, use the same steps as in Assigning Roles, but select the corresponding **Unassign** option in the Tasks panel.

Example

The scenario for this example is two office clerks responsible for updating information in the Genesys configuration, as follows:

- Clerk A is responsible for update the records for all employees, or User objects (both agents and non-agents).
- Clerk B is responsible for updating the list of skills, or Skill objects, that can be assigned to agents.

You want to use permissions and roles to ensure that each clerk has access to only the data they need to perform their job.

Permissions

Both clerks require Read/Write access permissions to their respective objects—Clerk A to Users, and Clerk B to Skills. Read access enables them to see the complete lists of objects, from which they can choose the specific object to be updated. Write access (the Change permission) enables them to update the objects.

Roles

Define specific roles as follows:

- HR_Clerk: Update information for all employees.
- Operations_Clerk: Update information for all skills that can be assigned to employees who are agents.

Create and configure each Role object with the appropriate role privileges, then assign each role to appropriate users as indicated in the following table:

Role	Role Privileges (as provided in Genesys Administrator)
HR_Clerk	Genesys Administrator - Modules > Provisioning = Allowed Genesys Administrator - Provisioning > Accounts = Allowed Genesys Administrator - Account Provisioning > Agent Info = Allowed Genesys Administrator - Account Provisioning > Users = Allowed
Operations_Clerk	Genesys Administrator - Modules > Provisioning = Allowed Genesys Administrator - Provisioning > Accounts = Allowed Genesys Administrator - Account Provisioning > Skills = Allowed

After the roles are assigned to users, only certain parts of the Genesys Administrator interface will be visible or available for use. The permissions assigned to each user determine what the user can do to or with the data displayed in those visible sections. In addition to the Provisioning tab, each clerk can see and do only the following:

- Clerk A:
  - View the Accounts section with only one item, Users.

  - View the full list of Users, from which he or she selects the User to be modified.
  - View and modify any property of the selected User.

> **Important**
>
> The Genesys Administrator > Account Provisioning > Agent Info = Allowed privilege enables the clerk to also modify information for agents.

- Clerk B:
  - View the Accounts section with only one item, Skills.
  - View the full list of Skills, from which he or she selects the Skill to be modified.
  - View and modify any property of the selected Skill.

Precautionary Notes

When configuring and using Role-Based Access Control, take note of the information in this section.

Searching for Objects

The Search facility in Genesys Administrator ignores any restrictions placed by roles, meaning that a user can view any object regardless of what roles they have been assigned. Therefore, in addition to roles, it is imperative that you also use permissions to prevent a user seeing objects for which they have no role privileges.

Hierarchical Access

When assigning a role to users, you must ensure that the lowest level object to which the role is intended to provide access is visible. In other words, if you grant access to an object inside one or more of the functional modules in Genesys Administrator (Monitoring, Provisioning, Deployment, and Operations), you must ensure that you also grant access to the appropriate modules themselves. See the table above to see how this is applied in the example.

For example, if you want to create a role that provides access to Places on the **Provisioning** tab, you must ensure that the users to whom this role will be assigned also have access to the Provisioning module. This can be done by defining and assigning two separate roles (one that grants access to the Provisioning module, and one that grants access to Places), or combined into one Role (one that grants access to both the Provisioning module and access to Places).

Assigning Roles to Individuals vs. Access Groups

Genesys strongly recommends that you avoid assigning a role to a large number of individual users directly. Instead, add the users to an access group and then assign the role to the access group. Assigning a role to a user directly is meaningful only if there are few administrative users for the role, for which it makes no sense to have an access group.